A Longitudinal and Comprehensive Study of the DANE Ecosystem in Email

Hyeonmin Lee, Aniketh Gireesh, Roland van Rijswijk-Deij, Taekyoung "Ted" Kwon, Taejoong Chung

Seoul National University, Amrita Vishwa Vidyapeetham, University of Twente & NLnet Labs, Virginia Polytechnic Institute and State University
The Problem of Public Key Infrastructure

• Some CAs were compromised and mis-issued fraudulent certificates for well-known domains
The Problem of Public Key Infrastructure

• Some CAs were compromised and mis-issued fraudulent certificates for well-known domains
  - e.g. CNNIC (2015), DigiNotar (2011), Comodo (2011), ...
The Problem of Public Key Infrastructure

- Some CAs were compromised and mis-issued **fraudulent certificates** for well-known domains
  - e.g. CNNIC (2015), DigiNotar (2011), Comodo (2011), ...

Can we trust all these CAs?
The Problem of Public Key Infrastructure

Suggested countermeasures

• Certificate Transparency (CT)
• Certification Authority Authorization (CAA)
• ...
The Problem of Public Key Infrastructure

Suggested countermeasures

• Certificate Transparency (CT)
• Certification Authority Authorization (CAA)
• ...

Do not fundamentally solve the problem!
Still rely on CAs
What is DANE?
DNS-based Authentication of Named Entities (DANE)

• An Internet security protocol which allows certificates to be bound to domain names
  - Publish certificate information as a DNS record (TLSA record)
DNS-based Authentication of Named Entities (DANE)

• An Internet security protocol which allows certificates to be bound to domain names
  - Publish certificate information as a DNS record (TLSA record)

• The Domain Name System Security Extensions (DNSSEC) is used to guarantee the integrity and authenticity of TLSA records
DNS-based Authentication of Named Entities (DANE)

• An Internet security protocol which allows certificates to be bound to domain names
  - Publish certificate information as a DNS record (TLSA record)

• The Domain Name System Security Extensions (DNSSEC) is used to guarantee the integrity and authenticity of TLSA records

Support TLS without relying on trusted third-parties like CAs
DNS-based Authentication of Named Entities (DANE)

DNS

root zone
Authoritative DNS server

.com zone
Authoritative DNS server

example.com zone
Publisher TLSA

TLSA records

TLS Server
(example.com)
DNS-based Authentication of Named Entities (DANE)

DNS

root zone
Authoritative DNS server

.com zone
Authoritative DNS server

example.com zone
Authoritative DNS server

① Fetch TLSA records

DNS Resolver

TLS Client

TLS Server
(example.com)

A Longitudinal and Comprehensive Study of the DANE Ecosystem in Email
DNS-based Authentication of Named Entities (DANE)

DNS (DNSSEC)

root zone
- root DNSKEY
  - RRSIG

.com zone
- .com DNSKEY
  - RRSIG
- DS
  - RRSIG
- example.com DNSKEY
  - RRSIG
  - RRSIG

example.com zone
- example.com DNSKEY
  - RRSIG

TLS Client

DNS Resolver

① Fetch TLSA records

TLS Server (example.com)

Authoritative DNS server

A Longitudinal and Comprehensive Study of the DANE Ecosystem in Email
DNS-based Authentication of Named Entities (DANE)

DNS (DNSSEC)

- root zone
  - root DNSKEY
  - RRSIG
- .com zone
  - .com DS
  - RRSIG
  - example.com DS
  - RRSIG
  - RRSIG
- example.com zone
  - example.com DNSKEY
  - RRSIG
  - example.com TLSA
  - RRSIG

1. Fetch TLSA records & RRSIG records

TLS Client

TLS Server (example.com)

Authoritative DNS server

A Longitudinal and Comprehensive Study of the DANE Ecosystem in Email
DNS-based Authentication of Named Entities (DANE)

1. Fetch TLSA records & RRSIG records
2. Validate DNSSEC Chain

A Longitudinal and Comprehensive Study of the DANE Ecosystem in Email
DNS-based Authentication of Named Entities (DANE)

DNS (DNSSEC)

1. Fetch TLSA records & RRSIG records
2. Validate DNSSEC Chain
3. Receive a certificate for TLS

A Longitudinal and Comprehensive Study of the DANE Ecosystem in Email
DNS-based Authentication of Named Entities (DANE)

DNS (DNSSEC)

root zone

- root DNSKEY
- RRSIG

.com zone

- .com DNSKEY
- RRSIG
- DS
- RRSIG

example.com zone

- example.com DNSKEY
- RRSIG
- example.com TLSA
- RRSIG

TLS Client

① Fetch TLSA records & RRSIG records

② Validate DNSSEC Chain

③ Receive a certificate for TLS

TLS Server
(example.com)

Authoritative DNS server
DNS-based Authentication of Named Entities (DANE)

DNS (DNSSEC)

1. Fetch TLSA records & RRSIG records

2. Validate DNSSEC Chain

3. Receive a certificate for TLS

4. Match TLSA records with the certificate

A Longitudinal and Comprehensive Study of the DANE Ecosystem in Email
DNS-based Authentication of Named Entities (DANE)

**DNS (DNSSEC)**
- root zone
  - root DNSKEY
  - RRSIG
- .com zone
  - .com DNSKEY
  - RRSIG
  - DS
  - RRSIG
- example.com zone
  - example.com DNSKEY
  - RRSIG
  - example.com TLSA
  - RRSIG

**Steps:**
1. **Fetch TLSA records & RRSIG records**
2. **Validate DNSSEC Chain**
3. **Receive a certificate for TLS**
4. **Match TLSA records with the certificate**
5. **TLS channel**

**Diagram:**
- DNS Resolver
- TLS Client
- TLS Server (example.com)
- Authoritative DNS server

**Overview:**
A Longitudinal and Comprehensive Study of the DANE Ecosystem in Email
Where DANE is used?
DANE + SMTP Background

• Simple Mail Transfer Protocol (SMTP) has no built-in security mechanism
DANE + SMTP Background

- Simple Mail Transfer Protocol (SMTP) has no built-in security mechanism
- STARTTLS supports opportunistic TLS for SMTP connection
DANE + SMTP Background

- Simple Mail Transfer Protocol (SMTP) has no built-in security mechanism
- STARTTLS supports opportunistic TLS for SMTP connection
DANE + SMTP Background

• Simple Mail Transfer Protocol (SMTP) has no built-in security mechanism

• STARTTLS supports opportunistic TLS for SMTP connection
DANE + SMTP Background

- Simple Mail Transfer Protocol (SMTP) has no built-in security mechanism
- STARTTLS supports opportunistic TLS for SMTP connection
DANE + SMTP Background

- Simple Mail Transfer Protocol (SMTP) has no built-in security mechanism
- STARTTLS supports opportunistic TLS for SMTP connection

Vulnerable to downgrade attacks
DANE + SMTP Background

- Simple Mail Transfer Protocol (SMTP) has no built-in security mechanism
- STARTTLS supports opportunistic TLS for SMTP connection

Vulnerable to downgrade attacks
With DANE, STARTTLS downgrade attack can be mitigated.

**DANE + SMTP**

With DANE, STARTTLS downgrade attack can be mitigated.
DANE + SMTP

- With DANE, STARTTLS downgrade attack can be mitigated

![Diagram showing DNSSEC with DANE keys and RRSIG records]

example.com supports STARTTLS!
DANE + SMTP

- How DANE + SMTP works?

1. Fetch TLSA records & RRSIG records
2. Validate DNSSEC Chain
3. Receive a certificate (through STARTTLS)
4. Match TLSA records with the certificate
5. Send an email over a TLS channel
DANE + SMTP

• How DANE + SMTP works?

1. Fetch **TLSA records** & **RRSIG records**
2. Validate **DNSSEC** Chain
3. Receive a **certificate** (through **STARTTLS**)
4. Match **TLSA records** with the **certificate**
5. Send an email over a TLS channel
Understanding of DANE Ecosystem

DNS Resolver

SMTP Client

Authoritative DNS server

SMTP Server
Understanding of DANE Ecosystem

- DNS Resolver
- Authoritative DNS server
- SMTP Client
- SMTP Server
Understanding of DANE Ecosystem

- DNS Resolver
- Authoritative DNS server
- SMTP Client
- SMTP Server

A Longitudinal and Comprehensive Study of the DANE Ecosystem in Email
Understanding of DANE Ecosystem

Server-side

- Publish TLSA records
- Support DNSSEC correctly

DNS Resolver

Authoritative DNS server

SMTP Client

SMTP Server

A Longitudinal and Comprehensive Study of the DANE Ecosystem in Email
Understanding of DANE Ecosystem

**Client-side**
- Fetch TLSA records
- Validate DNSSEC records

**Server-side**
- Publish TLSA records
- Support DNSSEC correctly

---

A Longitudinal and Comprehensive Study of the DANE Ecosystem in Email
Understanding of DANE Ecosystem

**Client-side**
- Fetch TLSA records
- Validate DNSSEC records

**Server-side**
- Publish TLSA records
- Support DNSSEC correctly
- Support STARTTLS

**DNS**
- DNS Resolver
- Authoritative DNS server

**SMTP**
- SMTP Client
- SMTP Server

---

A Longitudinal and Comprehensive Study of the DANE Ecosystem in Email
Understanding of DANE Ecosystem

Client-side
- Fetch TLSA records
- Validate DNSSEC records

Server-side
- Publish TLSA records
- Support DNSSEC correctly

DNS Resolver
- DNS
- Authoritative DNS server

SMTP Client
- SMTP
- Verify TLSA records with certificates

SMTP Server
- SMTP
- Support STARTTLS
Understanding of DANE Ecosystem

<table>
<thead>
<tr>
<th>Client-side</th>
<th>Server-side</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fetch TLSA records</td>
<td>Publish TLSA records</td>
</tr>
<tr>
<td>Validate DNSSEC records</td>
<td>Support DNSSEC correctly</td>
</tr>
<tr>
<td>Support STARTTLS</td>
<td>Support STARTTLS</td>
</tr>
<tr>
<td>Verify TLSA records with certificates</td>
<td></td>
</tr>
</tbody>
</table>

DANE can **only function correctly** when all entities fulfill their responsibilities.
Understanding of DANE Ecosystem

<table>
<thead>
<tr>
<th>Client-side</th>
<th>Server-side</th>
<th>Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fetch TLSA records</td>
<td>Publish TLSA records</td>
<td>Deployment</td>
</tr>
<tr>
<td>Validate DNSSEC records</td>
<td>Support DNSSEC correctly</td>
<td>TLSA</td>
</tr>
<tr>
<td>Support STARTTLS</td>
<td>Support STARTTLS</td>
<td>2 years Every Day</td>
</tr>
<tr>
<td>Verify TLSA records with certificates</td>
<td></td>
<td>5 TLD* .com, .net, .org .se, .nl</td>
</tr>
</tbody>
</table>

*OpenINTEL (https://openintel.nl/)

A Longitudinal and Comprehensive Study of the DANE Ecosystem in Email
Understanding of DANE Ecosystem

Client-side
- Fetch TLSA records
- Validate DNSSEC records
- Support STARTTLS
- Verify TLSA records with certificates

Server-side
- Publish TLSA records
- Support DNSSEC correctly
- Support STARTTLS

Analysis

Deployment
- TLSA
- 2 years
  Every Day
- 5 TLD*: .com, .net, .org .se, .nl

Management
- TLSA Certificate
- 4 months
  Every Hour

*OpenINTEL (https://openintel.nl/)

A Longitudinal and Comprehensive Study of the DANE Ecosystem in Email
Understanding of DANE Ecosystem

**Analysis**

**Client-side**
- Fetch TLSA records
- Validate DNSSEC records

**Server-side**
- Publish TLSA records
- Support DNSSEC correctly

**Popular Email Service Providers**

**Deployment**
- TLSA
  - 2 years
  - Every Day
- 5 TLD* (.com, .net, .org, .se, .nl)

**Management**
- TLSA Certificate
  - 4 months
  - Every Hour

*OpenINTEL ([https://openintel.nl/](https://openintel.nl/))

A Longitudinal and Comprehensive Study of the DANE Ecosystem in Email
## Understanding of DANE Ecosystem

### Analysis

<table>
<thead>
<tr>
<th>Popular Email Service Providers</th>
<th>Popular MTA and DNS Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Fetch TLSA records</td>
<td>- Support STARTTLS</td>
</tr>
<tr>
<td>- Validate DNSSEC records</td>
<td>- Verify TLSA records with certificates</td>
</tr>
</tbody>
</table>

### Client-side

- **DNS Resolver**
  - Fetch TLSA records
  - Validate DNSSEC records

### Server-side

- **Authoritative DNS server**
  - Publish TLSA records
  - Support DNSSEC correctly

- **SMTP Server**
  - Support STARTTLS

### Client-side (SMTP)

- **SMTP Client**
  - Fetch TLSA records
  - Validate DNSSEC records
  - Support STARTTLS
  - Verify TLSA records with certificates

### Analysis

- **Deployment**
  - TLSA
  - 2 years Every Day
  - 5 TLD* .com, .net, .org .se, .nl

- **Management**
  - TLSA Certificate
  - 4 months Every Hour

*OpenINTEL ([https://openintel.nl/](https://openintel.nl/))

---

**A Longitudinal and Comprehensive Study of the DANE Ecosystem in Email**
Outline of Analysis

**Server-side**

- DANE Deployment
- DANE Management

**Client-side**

- Email Service Provider
- MTA & DNS Software

A Longitudinal and Comprehensive Study of the DANE Ecosystem in Email
Outline of Analysis

Server-side

- DANE Deployment
- DANE Management

Client-side

- Email Service Provider
- MTA & DNS Software
DANE Deployment

• Deployment is rare, but steadily growing
DANE Deployment

• Deployment is rare, but steadily growing
DANE Deployment

• Deployment is rare, but steadily growing

• The deployment rate for .nl and .se is high
DANE Deployment

• Deployment is rare, but steadily growing

• The deployment rate for .nl and .se is high
  → Financial incentives from registries
DANE Deployment

• Deployment is rare, but steadily growing

• The deployment rate for .nl and .se is high
  → Financial incentives from registries

• Growth is mainly due to a small number of popular email service providers
DANE Deployment

• Deployment is rare, but steadily growing

• The deployment rate for .nl and .se is high
  → Financial incentives from registries

• Growth is mainly due to a small number of popular email service providers
DANE deployment is growing

0.6~0.7% (.com, .net, .org)  10% (.nl)  37% (.se)
DANE Deployment – Summary

DANE deployment is growing

0.6~0.7% (.com, .net, .org)  10% (.nl)  37% (.se)

Are they deployed DANE correctly?
Outline of Analysis

**Server-side**
- DANE Deployment
- DANE Management

**Client-side**
- Email Service Provider
- MTA & DNS Software

A Longitudinal and Comprehensive Study of the DANE Ecosystem in Email
Condition for Correct DANE Management

Support?

- **DS & RRSIG** records are published
Condition for Correct DANE Management

Support?

- DS & RRSIG records are published

- Certificates are provided

DNSSEC

STARTTLS
Condition for Correct DANE Management

**Support?**
- **DS & RRSIG** records are published
- **Certificates** are provided

**Correctly?**
- **DNSSEC** records are correct (e.g. not expired)
- **Certificates** are consistent with TLSA records
Condition for Correct DANE Management

Support?
- DS & RRSIG records are published
- Certificates are provided

Correctly?
- RRSIG records are correct (e.g. not expired)
- Certificates are consistent with TLSA records

Missing Components
- DNSSEC

Incorrect Components
- STARTTLS
Condition for Correct DANE Management

Support?

- DS & RRSIG records are published
- Certificates are provided

Correctly?

- RRSIG records are correct (e.g. not expired)
- Certificates are consistent with TLSA records

Missing Components

Incorrect Components

DNSSEC

STARTTLS

4 months / every hour
5 vantage points (Oregon, Virginia, São Paulo, Paris, Sydney)
Condition for Correct DANE Management

- DS & RRSIG records are published
- Certificates are provided
  - DNSSEC
  - STARTTLS

4 months / every hour
5 vantage points (Oregon, Virginia, São Paulo, Paris, Sydney)
→ No difference
Missing Components

85% are signed (have RRSIG record)
Missing Components

RRSIG ~ 15%
DS ~ 20%

85% are signed (have RRSIG record)

20% of them do not have DS records
Missing Components

85% are signed (have RRSIG record)

20% of them do not have DS records

99.7% supports STARTTLS
Missing Components

85% are signed (have RRSIG record)

20% of them do not have DS records

99.7% supports STARTTLS

0.01% of them provide no or malformed certificates

DNSSEC
- RRSIG ~ 15%
- DS ~ 20%

STARTTLS
- STARTTLS ~ 0.3%
- Certificate ~ 0.01%

A Longitudinal and Comprehensive Study of the DANE Ecosystem in Email
Missing Components

Main failure reason?

Missing DS records

rather than the absence of STARTTLS support

85% are signed (have RRSIG record)

99.7% supports STARTTLS

20% of them do not have DS records

0.01% of them provide no or malformed certificates
Incorrect Components

- **Incorrect Components**
  - **DNSSEC**
    - RRSIG ~ 15%
    - DS ~ 20%
  - **STARTTLS**
    - STARTTLS ~ 0.3%
    - Certificate ~ 0.01%
  - **Incorrect**
    - DNSSEC
    - Validation fail ~ 0.55%

- **Statistic**: 0.55% of DNSSEC records are *incorrect*
Incorrect Components

- **Missing**
  - DNSSEC
    - RRSIG ~ 15%
    - DS ~ 20%
  - STARTTLS
    - STARTTLS ~ 0.3%
    - Certificate ~ 0.01%

- **Incorrect**
  - DNSSEC
    - Validation fail ~ 0.55%
  - STARTTLS
    - Mismatch ~ 3.68%

- **Incorrect DNSSEC**
  - DNSSEC 0.55% of DNSSEC records are incorrect
  - STARTTLS 3.68% of certificates do not match with their corresponding TLSA records

A Longitudinal and Comprehensive Study of the DANE Ecosystem in Email
DANE Management – Summary

Mismanagement in the DANE ecosystem is pervasive

Missing or incorrect DNSSEC - 35%
Outline of Analysis

Server-side
- DANE Deployment
- DANE Management

Client-side
- Email Service Provider
- MTA & DNS Software
How many popular email service providers do support DANE and correctly?
Testbed

Authoritative DNS server

SMTP Server

BIND9

Postfix
Testbed

- Purchase a second-level domain name
  ex) dane-test.com
Testbed

- Purchase a second-level domain name
  ex) dane-test.com

- Set subdomains that are configured to different combination of DNSSEC, STARTTLS, and DANE misconfigurations
  ex) dnssec-expired-rrsig.dane-test.com
cert-tlsa-unmatched.dane-test.com
Testbed

- Purchase a second-level domain name
  ex) dane-test.com

- Set subdomains that are configured to different combination of DNSSEC, STARTTLS, and DANE misconfigurations
  ex) dnssec-expired-rrsig.dane-test.com
cert-tlsa-unmatched.dane-test.com

Test 29 popular*
email service providers

*Rank from Adobe’s leaked user email database (2013)
① Set up an email account (ex. Gmail)
Testbed

1. Set up an email account (ex. Gmail)
2. Send an email
Testbed

① Set up an email account (ex. Gmail)
② Send an email
③-1 MX and TLSA record lookup via DNS resolver
③-2 MX and TLSA record lookup

DNS resolver
SMTP Client
Authoritative DNS server
SMTP Server

A Longitudinal and Comprehensive Study of the DANE Ecosystem in Email
Testbed

① Set up an email account (ex. Gmail)
② Send an email
③-1 MX and TLSA record lookup via DNS resolver
③-2 MX and TLSA record lookup
④ Check DNSSEC lookup
⑤ Check TLSA lookup

A Longitudinal and Comprehensive Study of the DANE Ecosystem in Email
Testbed

1. Set up an email account (ex. Gmail)
2. Send an email

→ DNS

3.1 MX and TLSA record lookup via DNS resolver
3.2 MX and TLSA record lookup

4. Check DNSSEC lookup
5. Check TLSA lookup

6.1 Initiate an SMTP connection

SMTP Client

Authoritative DNS server

Testbed

SMTP Server
Testbed

1. Set up an email account (ex. Gmail)
2. Send an email

① Set up an email account (ex. Gmail)
② Send an email

③-1 MX and TLSA record lookup via DNS resolver
③-2 MX and TLSA record lookup

④ Check DNSSEC lookup
⑤ Check TLSA lookup

⑥-1 Initiate an SMTP connection
⑥-2 Check STARTTLS command

A Longitudinal and Comprehensive Study of the DANE Ecosystem in Email
A Longitudinal and Comprehensive Study of the DANE Ecosystem in Email

1. Set up an email account (ex. Gmail)
2. Send an email

① Set up an email account (ex. Gmail)
② Send an email

③-1 MX and TLSA record lookup via DNS resolver
③-2 MX and TLSA record lookup

④ Check DNSSEC lookup
⑤ Check TLSA lookup

⑥-1 Initiate an SMTP connection
⑥-2 Check STARTTLS command
⑥-3 Send a certificate

Testbed
A Longitudinal and Comprehensive Study of the DANE Ecosystem in Email
A Longitudinal and Comprehensive Study of the DANE Ecosystem in Email

① Set up an email account (ex. Gmail)
② Send an email
③-1 MX and TLSA record lookup via DNS resolver
③-2 MX and TLSA record lookup
④ Check DNSSEC lookup
⑤ Check TLSA lookup
⑥-1 Initiate an SMTP connection
⑥-2 Check STARTTLS command
⑥-3 Send a certificate
⑥-4 Check the established SMTP connection

ex) dnssec-expired-rrsig.dane-test.com
### Popular Email Service Providers’ DANE Support

<table>
<thead>
<tr>
<th>Mail Provider</th>
<th>DNSSEC Request (DNSKEY, DS)</th>
<th>Validation</th>
</tr>
</thead>
<tbody>
<tr>
<td>mail.com</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>comcast.net</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>gmx.com</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>tutanota.com</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>mynet.com</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>sapo.pt</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>sina.com</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>protonmail.com</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>aol.com</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>fastmail.com</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>freemail.hu</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>mail.ru</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>naver.com</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>rediffmail.com</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>yahoo.com</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>zoho.in</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>daum.net</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>interia.pl</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>inbox.lv</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>icloud.com</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>runbox.com</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>seznam.cz</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>o2.pl</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>wp.pl</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>sohu.com</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>t-online.de</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>excite.com</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>gmail.com</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>outlook.com</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

Total 29

**DNSSEC**

- Only 7 email providers actually fetch DNSKEY and DS records
### Popular Email Service Providers’ DANE Support

<table>
<thead>
<tr>
<th>Mail Provider</th>
<th>DNSSEC Request (DNSKEY, DS)</th>
<th>Validation</th>
</tr>
</thead>
<tbody>
<tr>
<td>mail.com</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>comcast.net</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>gmx.com</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>tutanota.com</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>mynet.com</td>
<td>✓</td>
<td>×</td>
</tr>
<tr>
<td>sapo.pt</td>
<td>✓</td>
<td>×</td>
</tr>
<tr>
<td>sina.com</td>
<td>✓</td>
<td>×</td>
</tr>
<tr>
<td>protonmail.com</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>aol.com</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>fastmail.com</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>freemail.hu</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>mail.ru</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>naver.com</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>reidffmail.com</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>yahoo.com</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>zoho.in</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>daum.net</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>interia.pl</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>inbox.lv</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>icloud.com</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>runbox.com</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>seznam.cz</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>o2.pl</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>wp.pl</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>sohu.com</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>t-online.de</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>excite.com</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>gmail.com</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>outlook.com</td>
<td>×</td>
<td>×</td>
</tr>
</tbody>
</table>

**Total 29**

**DNSSEC**

- Only 7 email providers actually fetch DNSKEY and DS records
- Only 4 providers correctly verify DNSSEC records

---

A Longitudinal and Comprehensive Study of the DANE Ecosystem in Email
### Popular Email Service Providers’ DANE Support

<table>
<thead>
<tr>
<th>Mail Provider</th>
<th>STARTTLS Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>mail.com</td>
<td>✓</td>
</tr>
<tr>
<td>comcast.net</td>
<td>✓</td>
</tr>
<tr>
<td>gmx.com</td>
<td>✓</td>
</tr>
<tr>
<td>tutanota.com</td>
<td>✓</td>
</tr>
<tr>
<td>mynet.com</td>
<td>✓</td>
</tr>
<tr>
<td>sapo.pt</td>
<td>✓</td>
</tr>
<tr>
<td>sina.com</td>
<td>x</td>
</tr>
<tr>
<td>protonmail.com</td>
<td>✓</td>
</tr>
<tr>
<td>aol.com</td>
<td>✓</td>
</tr>
<tr>
<td>fastmail.com</td>
<td>✓</td>
</tr>
<tr>
<td>freemail.hu</td>
<td>✓</td>
</tr>
<tr>
<td>mall.ru</td>
<td>✓</td>
</tr>
<tr>
<td>naver.com</td>
<td>✓</td>
</tr>
<tr>
<td>rediffmail.com</td>
<td>✓</td>
</tr>
<tr>
<td>yahoo.com</td>
<td>✓</td>
</tr>
<tr>
<td>zoho.in</td>
<td>✓</td>
</tr>
<tr>
<td>daum.net</td>
<td>✓</td>
</tr>
<tr>
<td>interia.pl</td>
<td>✓</td>
</tr>
<tr>
<td>inbox.lv</td>
<td>✓</td>
</tr>
<tr>
<td>icloud.com</td>
<td>✓</td>
</tr>
<tr>
<td>runbox.com</td>
<td>✓</td>
</tr>
<tr>
<td>seznam.cz</td>
<td>✓</td>
</tr>
<tr>
<td>o2.pl</td>
<td>x</td>
</tr>
<tr>
<td>wp.pl</td>
<td>x</td>
</tr>
<tr>
<td>sohu.com</td>
<td>x</td>
</tr>
<tr>
<td>t-online.de</td>
<td>x</td>
</tr>
<tr>
<td>excite.com</td>
<td>x</td>
</tr>
<tr>
<td>gmail.com</td>
<td>✓</td>
</tr>
<tr>
<td>outlook.com</td>
<td>✓</td>
</tr>
</tbody>
</table>

**Total 29**

**STARTTLS**

- 23 mail providers support STARTTLS
Popular Email Service Providers’ DANE Support

<table>
<thead>
<tr>
<th>Mail Provider</th>
<th>TLSA Request</th>
<th>Validation</th>
</tr>
</thead>
<tbody>
<tr>
<td>mail.com</td>
<td>✅</td>
<td></td>
</tr>
<tr>
<td>comcast.net</td>
<td>✅</td>
<td></td>
</tr>
<tr>
<td>gmx.com</td>
<td>✅</td>
<td></td>
</tr>
<tr>
<td>tutanota.com</td>
<td>✅</td>
<td>▲</td>
</tr>
<tr>
<td>mynet.com</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>sapo.pt</td>
<td>✗</td>
<td></td>
</tr>
<tr>
<td>sina.com</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>protonmail.com</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>aol.com</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>fastmail.com</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>freemail.hu</td>
<td>✗</td>
<td></td>
</tr>
<tr>
<td>mail.ru</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>naver.com</td>
<td>✗</td>
<td></td>
</tr>
<tr>
<td>rediffmail.com</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>yahoo.com</td>
<td>✗</td>
<td></td>
</tr>
<tr>
<td>zoho.in</td>
<td>✗</td>
<td></td>
</tr>
<tr>
<td>daum.net</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>interia.pl</td>
<td>✗</td>
<td></td>
</tr>
<tr>
<td>inbox.lv</td>
<td>✗</td>
<td></td>
</tr>
<tr>
<td>icloud.com</td>
<td>✗</td>
<td></td>
</tr>
<tr>
<td>runbox.com</td>
<td>✗</td>
<td></td>
</tr>
<tr>
<td>seznam.cz</td>
<td>✗</td>
<td></td>
</tr>
<tr>
<td>o2.pl</td>
<td>✗</td>
<td></td>
</tr>
<tr>
<td>wp.pl</td>
<td>✗</td>
<td></td>
</tr>
<tr>
<td>sohu.com</td>
<td>✗</td>
<td></td>
</tr>
<tr>
<td>t-online.de</td>
<td>✗</td>
<td></td>
</tr>
<tr>
<td>excite.com</td>
<td>✗</td>
<td></td>
</tr>
<tr>
<td>gmail.com</td>
<td>✗</td>
<td></td>
</tr>
<tr>
<td>outlook.com</td>
<td>✗</td>
<td></td>
</tr>
</tbody>
</table>

Total 29

DANE

- 4 mail providers fetch TLSA records
## Popular Email Service Providers’ DANE Support

<table>
<thead>
<tr>
<th>Mail Provider</th>
<th>TLSA Request</th>
<th>Validation</th>
</tr>
</thead>
<tbody>
<tr>
<td>mail.com</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>comcast.net</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>gmx.com</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>tutanota.com</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>mynet.com</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>sapo.pt</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>sina.com</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>protonmail.com</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>aol.com</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>fastmail.com</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>freemail.hu</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>mail.ru</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>naver.com</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>rediffmail.com</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>yahoo.com</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>zoho.in</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>daum.net</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>interia.pl</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>inbox.lv</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>icloud.com</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>runbox.com</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>seznam.cz</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>o2.pl</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>wp.pl</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>sohu.com</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>t-online.de</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>excite.com</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>gmail.com</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>outlook.com</td>
<td>×</td>
<td>×</td>
</tr>
</tbody>
</table>

**Total 29**

**DANE**

- 4 mail providers fetch TLSA records
- 2 providers correctly validate all fields in a TLSA record
### Popular Email Service Providers’ DANE Support

<table>
<thead>
<tr>
<th>Mail Provider</th>
<th>TLSA Request</th>
<th>Validation</th>
</tr>
</thead>
<tbody>
<tr>
<td>mail.com</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>comcast.net</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>gmx.com</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>tutanota.com</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>mynet.com</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>sapo.pt</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>sina.com</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>protonmail.com</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>aol.com</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>fastmail.com</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>freemail.hu</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>mail.ru</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>naver.com</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>rediffmail.com</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>yahoo.com</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>zoho.in</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>daum.net</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>interia.pl</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>inbox.lv</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>icloud.com</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>runbox.com</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>seznam.cz</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>o2.pl</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>wp.pl</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>sohu.com</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>t-online.de</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>excite.com</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>gmail.com</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>outlook.com</td>
<td>✗</td>
<td>✗</td>
</tr>
</tbody>
</table>

Total 29

#### DANE

- 4 mail providers fetch TLSA records
- 2 providers **correctly validate** all fields in a TLSA record
- Other 2 providers **do not validate** one field correctly
Popular Email Service Providers’ DANE Support

DANE support in the popular email service providers is still in an early stage
Outline of Analysis

Server-side

DANE Deployment

DANE Management

Client-side

Email Service Provider

MTA & DNS Software

A Longitudinal and Comprehensive Study of the DANE Ecosystem in Email
## Popular MTA and DNS software

<table>
<thead>
<tr>
<th>MTA Software</th>
<th>STARTTLS Support</th>
<th>DANE Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Postfix 3.4.7</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Exim 4.92.3</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>sendmail 8.15.2</td>
<td>✓</td>
<td>✘</td>
</tr>
<tr>
<td>Exchange Server 2019</td>
<td>✓</td>
<td>✘</td>
</tr>
</tbody>
</table>

All support STARTTLS
2 support DANE
### Popular MTA and DNS software

<table>
<thead>
<tr>
<th>MTA Software</th>
<th>STARTTLS Support</th>
<th>DANE Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Postfix 3.4.7</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Exim 4.92.3</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>sendmail 8.15.2</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Exchange Server 2019</td>
<td>✓</td>
<td>✗</td>
</tr>
</tbody>
</table>

All support STARTTLS
2 support DANE

<table>
<thead>
<tr>
<th>DNS Software</th>
<th>DNSSEC Support</th>
<th>TLSA Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIND9 9.14.7</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>PowerDNS 4.2.0</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Microsoft DNS</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Simple DNS Plus 8.0.110</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>NSD 4.2.2</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>KnotDNS 2.9.0</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>YADIFA 2.3.9</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Unbound 1.9.4</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>djbdns 1.05</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>MaraDNS 3.4.01</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>posadis 0.60.6</td>
<td>✗</td>
<td>✗</td>
</tr>
</tbody>
</table>

8 support DNSSEC
TLSA
Popular MTA and DNS software

DANE support in the popular MTA and DNS programs is pervasive
Conclusion

• Presented a longitudinal and comprehensive study of the DANE ecosystem in SMTP

• Server-side: DANE deployment is scarce but increasing
  - 1/3 of TLSA records cannot be validated due to missing or incorrect DNSSEC records
  - 3.68% of the certificates are inconsistent with their TLSA records

• Client-side: DANE deployment is also rare
  - Only 4 email service providers support DANE out of 29 popular email providers
  - 2 MTA and 8 DNS programs support DANE

• Datasets & source code
  - https://dane-study.github.io/
Thank you!

Any questions?

Hyeonmin Lee
hmlee@mmlab.snu.ac.kr
Appendix
## DANE Deployment – Daily Dataset

Domain data from OpenINTEL (https://openintel.nl/)

<table>
<thead>
<tr>
<th>TLD</th>
<th>Generic TLD</th>
<th>Country-code TLD</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>.com</td>
<td>.org</td>
</tr>
<tr>
<td># of scanned domains</td>
<td>72.9M</td>
<td>7.4M</td>
</tr>
<tr>
<td>Interval</td>
<td>2017-10-22</td>
<td>2019-10-31</td>
</tr>
<tr>
<td>Period</td>
<td>Every day</td>
<td></td>
</tr>
</tbody>
</table>
## DANE Management – Hourly Dataset

<table>
<thead>
<tr>
<th>Vantage Point</th>
<th>Oregon</th>
<th>Virginia</th>
<th>São Paulo</th>
<th>Paris</th>
<th>Sydney</th>
</tr>
</thead>
<tbody>
<tr>
<td># of TLSA records (of last snapshot)</td>
<td>7.9K</td>
<td>7.9K</td>
<td>7.9K</td>
<td>7.9K</td>
<td>7.9K</td>
</tr>
<tr>
<td># of Certificates (of last snapshot)</td>
<td>7.3K</td>
<td>7.3K</td>
<td>7.3K</td>
<td>7.3K</td>
<td>7.2K</td>
</tr>
<tr>
<td>Interval</td>
<td>2019-07-11 ~ 2019-10-31</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Period</td>
<td>Every Hour</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>